IN THE UNITED STATES PATENT AND TRADEMARKS OFFICE

In The Matter of Patent Application:

First Named Inventor	:	Hamid Ould-Brahim
Serial No.	:	10/658,701
Filing Date	:	September 9, 2003
Title	:	SVC-L2 VPNs: FLEXIBLE ON DEMAND SWITCHED MPLS/IP LAYER-2 VPNs FOR ETHERNET SVC, ATM AND FRAME RELAY
Examiner	:	CHEA, PHILIP J
Art Unit	:	2453
Confirmation No.	:	2312

To: Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF ON APPEAL

Dear Sir:

This Appeal Brief is submitted further to the Notice of Appeal From The Examiner To The Board Of Patent Appeals And Interferences filed January 7, 2010. The Applicant respectfully submits that this Appeal Brief complies with all requirements of 37 C.F.R. 41.37.

The fee for filing this Appeal Brief is submitted herewith. In the Applicant's respectful submission, no other fees are due in connection with the filing of this Appeal Brief. If the Applicant is mistaken, the Commissioner is hereby authorized to deduct any fees required, and, in particular, any extension of time fees, from deposit account no.

13-2400.

TABLE OF CONTENTS

Real Party in Interest ..... page 3
Related Appeals and Interferences ..... page 3
Status of Claims ..... page 3
Status of Amendments ..... page 3
Summary of Claimed Subject Matter ..... page 4
Grounds of Rejection to be Reviewed on Appeal ..... page 6
Argument ..... page 7
Claims Appendix ..... page 17
Evidence Appendix ..... page 22
Related Proceedings Appendix ..... page 23

(i) *Real party in interest*

The real party in interest is Nortel Networks Limited, 2351 Boulevard Alfred-Nobel, St. Laurent, Quebec, H4S 2A9, Canada. Nortel Networks Limited is the Assignee of the entire right, title and interest in the subject application, by virtue of an Assignment recorded on 09/09/2003 on Reel 014487 at Frame 0282.

(ii) *Related appeals and interferences*

Appellant, the undersigned Agent, and Assignee are not aware of any related appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(iii) *Status of claims*

Claims 1-17 remain pending in the application. Claims 1-17 stand as originally filed. Each of claims 1-17 has been rejected. A copy of the pending claims as they currently stand finally rejected is attached as the Claims Appendix.

(iv) *Status of amendments*

Amendments were filed responsive to the final Office Action of October 8, 2009. According to the Advisory Action of December 16, 2009, the amendments have not been entered.

(v) *Summary of claimed subject matter*

Claim 1 is an independent claim to a network for providing switched virtual circuit Layer-2 VPNs. The claimed network includes a set of elements interconnected by services. At least one first subset of the elements (201, 202, 206, Page 6, line 26 to page 7, line 3) define a private network. At least one second subset of the elements (FIG. 2, elements 210, 212, 214, 215, 216, 217, 218, page 6, line 21-25) different from the first subset define a provider network wherein at least two subgroups of the first subset of elements may be connected via the provider network. A provisioning mechanism (page 8, lines 12-20 and page 12, lines 1-6) is used to define element membership in the first subset of elements. A plurality of customer ports (FIG. 3, 304, page 11, lines 24-29) are maintained on the elements of the first subset of elements. A plurality of provider ports (FIG. 3, 302, page 12, lines 1-6) are maintained on the second set of elements, each of the plurality of provider ports connected by data and signalling services to a customer port. A port information table (FIG. 4, 405, 407, page 14, lines 16-21) is present at each element of the provider network having a provider port, the port information table containing mapping information relating addresses of customer ports to addresses of provider ports for the first subset of elements. A signalling mechanism (page 10, lines 26-28) is used to create Layer-2 connectivity between elements within the first subset of elements at the Layer-2 level across the second subset of elements.

Claim 9 is an independent claim to a method of organizing a network having a set of elements interconnected by services, wherein at least one first subset of the elements defines a private network and at least one second subset of elements, different from the first subset, defines a provider network and wherein at least two subgroups of the first subset of elements may be connected via the provider network. The method includes defining element membership in the first subset of elements via a provisioning mechanism (page 10, lines 11-13) and establishing (page 8, lines 12-20) a plurality of customer ports (FIG. 3, 304) within the elements of the first subset of elements. The method also includes establishing (page 12, lines 1-6) a plurality of provider ports (FIG. 3, 302) within the second set of elements, each of the plurality of provider ports connected by data and signalling services to a customer port and establishing (page 14, lines 16-21) a port information table (FIG. 4, 405, 407) at each element of the provider network having a provider port, the port information table containing mapping information relating addresses of customer ports to addresses of provider ports. The method even further includes creating Layer-2 connectivity (page 10, lines 26-28) within the first subset of elements at the Layer-2 level across the second subset of elements via a signalling mechanism.

Claim 17 is an independent claim to a method of organizing a network having a set of elements interconnected by services, wherein at least one first subset of the elements defines a private network and at least one second subset of elements different from the first subset defines a provider network and wherein at least two

subgroups of the first subset of elements may be connected via the provider network. The method includes defining a L2VPN topology (page 10, line 26 to page 11, line 3). The method also includes establishing (page 8, lines 12-20) a plurality of customer ports (FIG. 3, 304) within the elements of the first subset of elements and establishing (page 12, lines 1-6) a plurality of provider ports (FIG. 3, 302) within the second set of elements, each of the plurality of provider ports connected by data and signalling services to a customer port. The method further includes creating (page 14, lines 16-21) a Layer-2 port information table (FIG. 4, 405, 407) for each provider port, establishing the identity (page 13, line 7) of customer ports attached to each provider port, and populating (page 13, line 8) the Layer-2 Port Information Table at that provider port with mapping information relating addresses of customer ports to addresses of provider ports. The method even further includes distributing (page 13, line 28 to page 14, line 3) the mapping information to Layer-2 Port Information Tables of the provider network via an auto-discovery mechanism and creating Layer-2 connectivity (page 10, lines 26-28) within the first subset of elements at the Layer-2 level across the second subset of elements via a signalling mechanism upon request from an element within the first subset of elements.

(vi) *Grounds of rejection to be reviewed on appeal*

Issues

The following issues are on appeal:

Whether claims 8 and 16 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over US Patent 6,662,221 to Gonda et al. (hereinafter "Gonda") in view of US Patent Application Publication No. 2002/0032766 to Xu et al. (hereinafter "Xu"). Claims 8 and 16 are on appeal.

(vii) *Argument*

Overview of Claimed Invention

The claimed invention relates to a Layer-2 virtual private network (VPN) arrangement and method for switched virtual circuits. The switched virtual circuit Layer-2 VPN includes logical ports of two types, customer and provider, and port information tables to relate both types. The port information tables provide simplified provisioning and a degree of customer autonomy regarding establishing virtual connections without the assistance of the service provider across the service provider's network. The switched virtual circuit Layer-2 VPN is particularly useful for overcoming the need for customers to store and manipulate provider addresses with respect to closed user groups, as is done in existing Layer-2 VPNS.

Overview of Primary Cited Art

Gonda discloses an automated system for managing a virtual private network. The system comprises one or more processing devices operative to: (i) generate a service order based on a request from a user for at least one of a new service, a modification of an existing service and a termination of an existing service

associated with the virtual private network; (ii) cause a determination of design requirements associated with implementing the user's request; (iii) cause provisioning of one or more virtual private network elements, when necessary, to implement the design requirements; (iv) cause the virtual private network to be configured to satisfy one or more conditions associated with the user's request; and (v) cause at least a portion of the virtual private network to be tested to determine whether the user's request has been satisfied; and a memory, coupled to the one or more processing devices, which stores at least a portion of data associated with the generating, design, provisioning, configuration and testing operations.

Xu describes methods and systems of delivering a network service. In one embodiment of Xu, a data packet including a service address and a payload is received. A plurality of network applications associated with the service address of the data packet are identified. The plurality of network applications associated with the service address include a first network application, a second network application, and a third network application. At least the payload of the data packet is sent to the first network application and the second network application. A second network application response packet is received from the second network application. A third network application packet is sent to the third network application, and the third network application packet is based at least in part on the second network application response packet.

Argument Regarding Rejections

The Examiner has rejected claims 8 and 16 under 35 U.S.C. § 103(a) as being obvious having regard to Gonda in view of Xu.

The Final Office Action was issued following the United States Supreme Court's decision in the case of KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398 (2007). In light of the KSR decision, Applicant wishes to address various issues pertaining to a proper analysis under section 103.

The Examiner, by citing two references and asserting a reason for combining elements from the two references, has elected to base the rejection of claims 8 and 16 upon a teaching, suggestion or motivation to select and combine features from the cited references. Applicant wishes to point out that the Supreme Court's KSR decision did not reject use of a "teaching, suggestion or motivation" analysis as part of an obviousness analysis, characterizing the analysis as "a helpful insight." KSR slip op. at 14-15.

When the Examiner chooses to base a rejection upon a teaching, suggestion or motivation analysis, the Examiner must satisfy the requirements of such an analysis. In particular, the Examiner must demonstrate with evidence and reasoned argument that there was a teaching, suggestion or motivation to select and combine features from the cited references, e.g., In re Lee, 61 USPQ2d 1430, 1433 (Fed. Cir. 2002). Moreover, the prior art must suggest the desirability of the combination, not

merely the feasibility, see In re Fulton, 73 USPQ2d 1141, 1145 (Fed. Cir. 2004).

In the event that the cited references fail to disclose or suggest all of the elements recited in the claims, then combining elements from the references would not yield the claimed subject matter, regardless of the extent of any teaching, suggestion or motivation.

Although the Supreme Court did not reject use of a "teaching, suggestion or motivation" analysis, the Supreme Court did say that it was not the only possible analysis of an obviousness question. Because of the Examiner's chosen ground for rejection, however, the only pending ground for rejection must be a "teaching, suggestion or motivation" analysis. In the event that the Examiner chooses to consider a different avenue for rejection, this would be a new ground for rejection not due to any action by Applicant. Applicant has a right to be heard on any new ground for rejection.

Applicant further respectfully reminds the Examiner that, even after KSR, the following legal principles are still valid, having been endorsed by the Supreme Court or having been unaffected by its decision: (1) the USPTO still has the burden of proof on the issue of obviousness; (2) the USPTO must base its decision upon evidence, and it must support its decision with articulated reasoning (slip op. at 14); (3) merely demonstrating that all elements of the claimed invention exist in the prior art is not sufficient to support a determination of obviousness (slip op. at 14-15); (4) hindsight has no place in an obviousness analysis (slip op. at 17); and (5) Applicant is entitled to a

careful, thorough, professional examination of the claims (slip op. at 7, 23, in which the Supreme Court remarked that a poor examination reflected poorly upon the USPTO).

Claim 8

It appears that the Examiner's rationale for the rejection of claim 8 is that claim 8 combines prior art elements according to known methods to yield predictable results. The Applicant respectfully submits that the references cited by the Examiner fail to disclose or suggest all of the elements recited in claim 8.

Claim 1, on which claim 8 depends, requires "a port information table at each element of said provider network having a provider port, said port information table containing mapping information relating addresses of customer ports to addresses of provider ports for said first subset of elements". The Examiner has indicated that Gonda discloses such a port information table in column 14, at lines 26-36.

The Applicant submits that a Graphical User Interface ("GUI") screen associated with management of a service order is distinct from a port information table "containing mapping information relating addresses of customer ports to addresses of provider ports" as required by claim 1. In prosecution, the Examiner has maintained that the mapping of a "customer premise equipment port number" to a "network access server/switch port number" that is present in the order management GUI of FIG. 10D of Gonda is read on by addresses of ports as claimed.

The Applicant submits that the limitations of claim 8 clarify that the addresses in the port information table of claim 8, by virtue of dependence on claim 1, are distinct from the port numbers in the order management GUI of Gonda.

The Examiner admits that Gonda fails to disclose that the customer port addresses and provider port addresses use an addressing scheme chosen from the group of IPv4, IPv6 and NSAP, as provided by the limitation of claim 8. The Examiner then cites Xu to illustrate that IPv4 and IPv6 addressing schemes may be used for IP addresses and service ports. However, the Applicant submits that Xu does not disclose use of IPv4 and IPv6 addressing schemes **for ports**. Instead, Xu proposes, in paragraph [0091], "assigning a service identifier associated with the pseudo network address that corresponds to the subset or package of network applications". Put another way, Xu proposes that a package of network applications be associated with pseudo network address and a service identifier. From paragraph [0092], "the service identifier comprises a conventional TCP/UDP service port". See also FIG. 5J where a packet is associated with a destination IP address and a service port. Furthermore, paragraph [0106] of Xu includes the passage "In these Figures, the packet routing is indicated in the form: IP(X,Y,Z), where X is the source IP address, Y is the destination IP address, and Z is the TCP port number."

So, in Xu, a given package of network applications may be associated with pseudo network address UUU.VVV.WWW.XXX and a service identifier YYY, i.e.,

UUU.VVV.WWW.XXX:YYY.

In contrast, in view of FIG. 4 of the present application, Layer2 Port Information Table 405 shows four address pairs and additional information for VPN A. One example address pair includes a Customer Port Identifier (CPI) of "10.1.1.1" and a Provider Port Identifier (PPI) of "16.1.1.2". Clearly, an IPv4 addressing scheme is being used here for customer port addresses and provider port addresses in a manner distinct from that disclosed in Xu.

Since neither Gonda, nor Xu, nor a combination of Gonda and Xu suggest or disclose "a port information table at each element of said provider network having a provider port, said port information table containing mapping information relating addresses of customer ports to addresses of provider ports for said first subset of elements" "wherein said customer port addresses and provider port addresses use an addressing scheme chosen from the group of IPv4, IPv6 and NSAP" as required by claim 8, the Applicant submits that the Examiner has erred in rejecting claim 8 as an obvious combination of Gonda and Xu.

Claim 16

It appears that the Examiner's rationale for the rejection of claim 16 is that claim 16 combines prior art elements according to known methods to yield predictable results. The Applicant respectfully submits that the references cited by the Examiner fail to disclose or suggest all of the elements recited in claim 16.

Claim 9, on which claim 16 depends, requires "establishing a port information table at each element of said provider network having a provider port, said port information table containing mapping information relating addresses of customer ports to addresses of provider ports". The Examiner has indicated that Gonda discloses such a port information table in column 14, at lines 26-36.

The Applicant submits that a GUI screen associated with management of a service order is distinct from a port information table "containing mapping information relating addresses of customer ports to addresses of provider ports" as required by claim 1. In prosecution, the Examiner has maintained that the mapping of a "customer premise equipment port number" to a "network access server/switch port number" that is present in the order management GUI of FIG. 10D of Gonda is read on by addresses of ports as claimed.

The Applicant submits that the limitations of claim 16 clarify that the addresses in the port information table of claim 16, by virtue of dependence on claim 9, are distinct from the port numbers in the order management GUI of Gonda.

The Examiner admits that Gonda fails to disclose that the customer port addresses and provider port addresses use an addressing scheme chosen from the group of IPv4, IPv6 and NSAP, as provided by the limitation of claim 16. The Examiner then cites Xu to illustrate that IPv4 and IPv6 addressing schemes may be used for IP addresses and service ports. However, the Applicant submits that Xu does not disclose

use of IPv4 and IPv6 addressing schemes for ports. Instead, Xu proposes, in paragraph [0091], "assigning a service identifier associated with the pseudo network address that corresponds to the subset or package of network applications". Put another way, Xu proposes that a package of network applications be associated with pseudo network address and a service identifier. See also FIG. 5J where a packet is associated with a destination IP address and a service port. Furthermore, paragraph [0106] of Xu includes the passage "In these Figures, the packet routing is indicated in the form: IP(X,Y,Z), where X is the source IP address, Y is the destination IP address, and Z is the TCP port number."

So, in Xu, a given package of network applications may be associated with pseudo network address UUU.VVV.WWW.XXX and a service identifier YYY, i.e., UUU.VVV.WWW.XXX:YYY.

In contrast, in view of FIG. 4 of the present application, Layer2 Port Information Table 405 shows four address pairs and additional information for VPN A. One example address pair includes a Customer Port Identifier (CPI) of "10.1.1.1" and a Provider Port Identifier (PPI) of "16.1.1.2". Clearly, an IPv4 addressing scheme is being used here for customer port addresses and provider port addresses in a manner distinct from that disclosed in Xu.

Since neither Gonda, nor Xu, nor a combination of Gonda and Xu suggest or disclose "establishing a port information table at each element of said provider

network having a provider port, said port information table containing mapping information relating addresses of customer ports to addresses of provider ports" "wherein said customer port addresses and provider port addresses use an addressing scheme chosen from the group of IPv4, IPv6 and NSAP" as required by claim 16, the Applicant submits that the Examiner has erred in rejecting claim 16 as an obvious combination of Gonda and Xu.

Conclusion

In conclusion, the Examiner's rejections of claims 8 and 16 under 35 U.S.C. § 103(a) fail to establish a *prima facie* case of obviousness. The rejections are therefore improper and the Appellant respectfully requests that the Board reverse the Examiner's obviousness rejections of claims 8 and 16.

Respectfully Submitted,
Hamid Ould-Brahim

By: /Colin Climie/
Colin Climie
Registration No. 56,036

Place: Toronto, Ontario, Canada
Date: March 5, 2010
Tele No.: 416-865-1482

(viii) *Claims Appendix*

1. (rejected) A network for providing switched virtual circuit Layer-2 VPNs, said network comprising:

a set of elements interconnected by services;

at least one first subset of said elements defining a private network;

at least one second subset of elements different from said first subset defining a provider network wherein at least two subgroups of said first subset of elements may be connected via said provider network;

a provisioning mechanism used to define element membership in said first subset of elements;

a plurality of customer ports maintained on said elements of said first subset of elements;

a plurality of provider ports maintained on said second set of elements, each of said plurality of provider ports connected by data and signalling services to a customer port;

a port information table at each element of said provider network having a provider port, said port information table containing mapping information relating addresses of customer ports to addresses of provider ports for said first subset of elements; and

a signalling mechanism used to create Layer-2 connectivity between elements within said first subset of elements at the Layer-2 level across said second subset of elements.

2. (rejected) A network for providing switched virtual circuit Layer-2 VPNs as claimed in claim 1, wherein said signalling mechanism is an MPLS signalling mechanism.

3. (rejected) A network for providing switched virtual circuit Layer-2 VPNs as claimed in claim 1, further comprising an auto-discovery mechanism for distributing said mapping information to port information tables of said provider network.

4. (rejected) A network for providing switched virtual circuit Layer-2 VPNs as claimed in claim 3, wherein said auto-discovery mechanism for distributing said mapping information uses Border Gateway Protocol.

5. (rejected) A network for providing switched virtual circuit Layer-2 VPNs as claimed in claim 1, wherein said provisioning mechanism operates in conjunction with said signalling mechanism to restrict element connectivity to elements of said first subset.

6. (rejected) A network for providing switched virtual circuit Layer-2 VPNs as claimed in claim 1, wherein said data and signalling services have IP signalling services.

7. (rejected) A network for providing switched virtual circuit Layer-2 VPNs as claimed in claim 1, wherein said customer port addresses need be unique only within said first subset of elements.

8. (rejected) A network for providing switched virtual circuit Layer-2 VPNs as claimed in claim 1, wherein said customer port addresses and provider port addresses use an addressing scheme chosen from the group of IPv4, IPv6, and NSAP.

9. (rejected) A method of organizing a network having a set of elements interconnected by services, wherein at least one first subset of said elements defines a private network and at least one second subset of elements different from said first subset defines a provider network and wherein at least two subgroups of said first subset of elements may be connected via said provider network, said method comprising:

defining element membership in said first subset of elements via a provisioning mechanism;

establishing a plurality of customer ports within said elements of said first subset of elements;

establishing a plurality of provider ports within said second set of elements, each of said plurality of provider ports connected by data and signalling services to a customer port;

establishing a port information table at each element of said provider network having a provider port, said port information table containing mapping information relating addresses of customer ports to addresses of provider ports; and

creating Layer-2 connectivity within said first subset of elements at the Layer-2 level across said second subset of elements via a signalling mechanism.

10. (rejected) The method of claim 9 wherein said signalling mechanism is an MPLS signalling mechanism.

11. (rejected) The method of claim 9, further comprising the step of: distributing said mapping information to port information tables of said provider network via an auto-discovery mechanism.

12. (rejected) The method of claim 11, wherein said auto-discovery mechanism for distributing said mapping information uses Border Gateway Protocol.

13. (rejected) The method of claim 9 further comprising the step of: restricting element connectivity to elements of said first subset via said provisioning mechanism operating in conjunction with said signalling mechanism.

14. (rejected) The method of claim 9 wherein said data and signalling services have IP signalling services.

15. (rejected) The method of claim 9 wherein said customer port addresses need be unique only within said first subset of elements.

16. (rejected) The method of claim 9 wherein said customer port addresses and provider port addresses use an addressing scheme chosen from the group of IPv4, IPv6, and NSAP.

17. (rejected) A method of organizing a network having a set of elements interconnected by services, wherein at least one first subset of said elements defines a private network and at least one second subset of elements different from said first subset defines a provider network and wherein at least two subgroups of said first subset of elements may be connected via said provider network, said method comprising:

defining a L2VPN topology;

establishing a plurality of customer ports within said elements of said first subset of elements;

establishing a plurality of provider ports within said second set of elements, each of said plurality of provider ports connected by data and signalling services to a customer port;

creating a Layer-2 Port Information Table for each provider port;

establishing the identity of customer ports attached to each provider port, and populating the Layer-2 Port Information Table at that provider port with mapping information relating addresses of customer ports to addresses of provider ports;

distributing said mapping information to Layer-2 Port Information Tables of said provider network via an auto-discovery mechanism; and

creating Layer-2 connectivity within said first subset of elements at the Layer-2 level across said second subset of elements via a signalling mechanism upon request from an element within said first subset of elements.

(ix) *Evidence Appendix*

None.

(x) *Related Proceedings Appendix*

None.